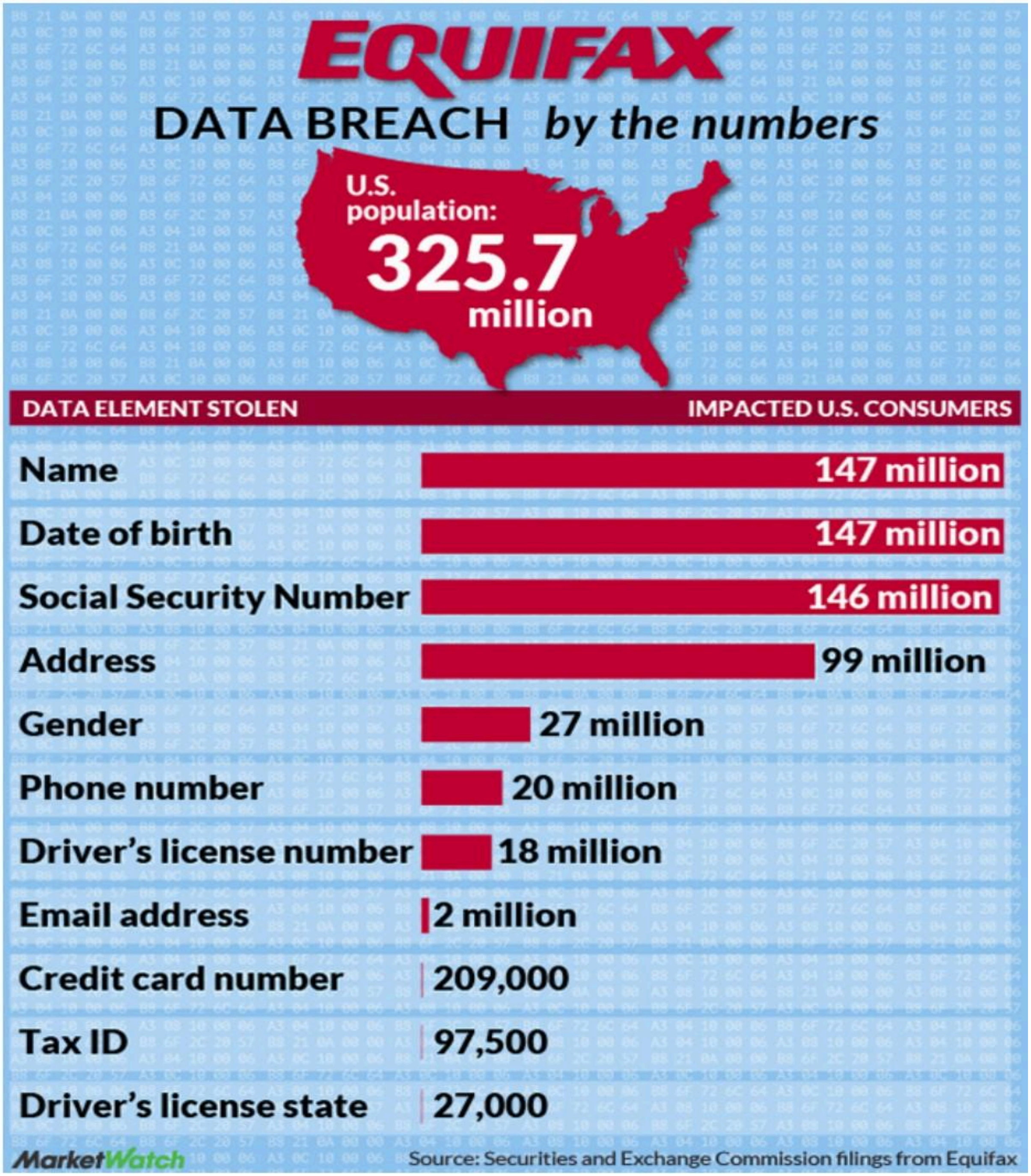
Equifax Data Breach

(Part 1)

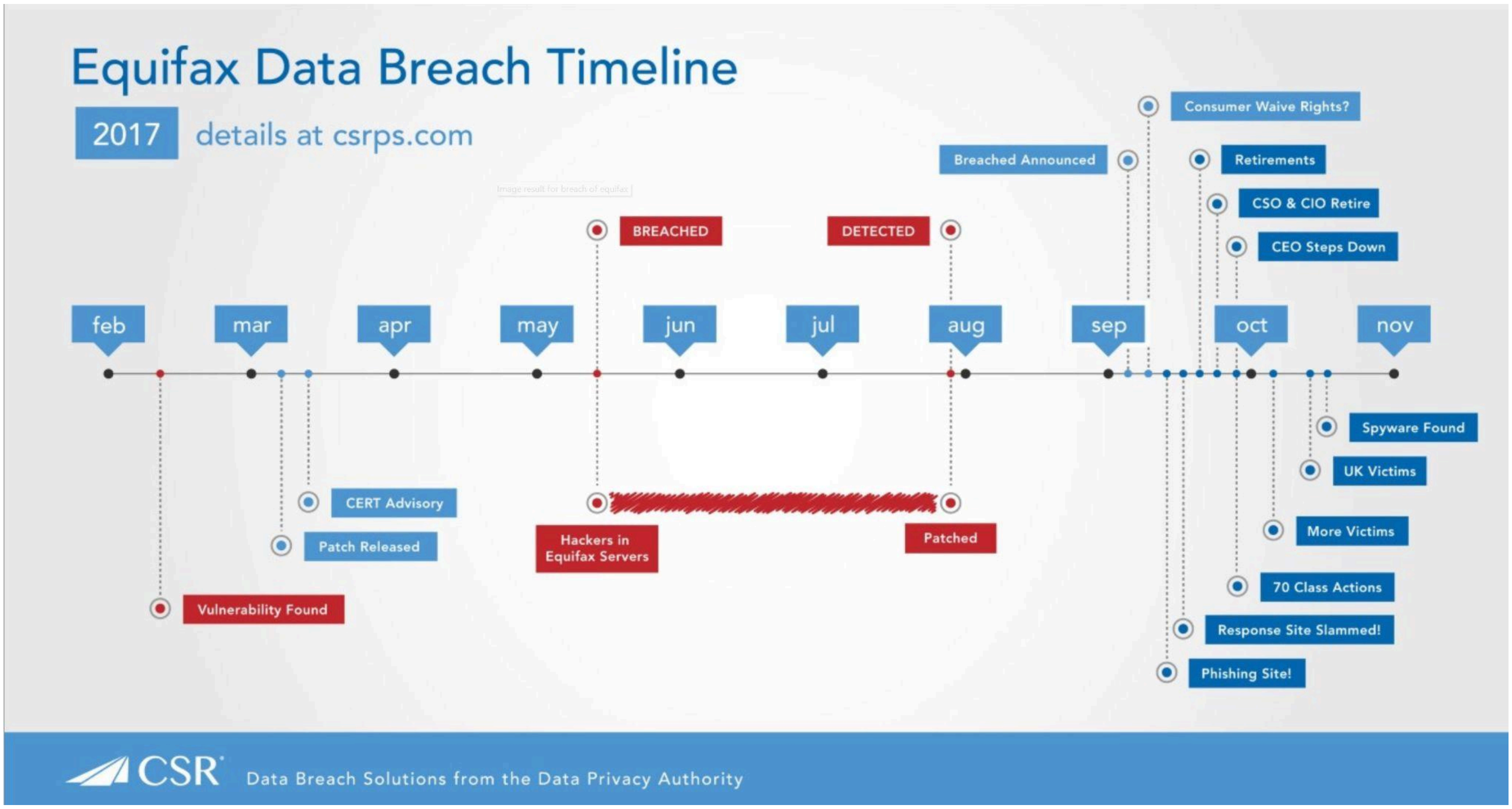
Overview:

Equifax, one of the three largest consumer credit reporting agencies, announced in September 2017 that its systems had been breached and that the sensitive data of 147 million Americans had been compromised.



Source: Securities and Exchange Commission filings from Equifax

The Timeline:



Cybersecurity Risk Management Failures:

- **Patch Management Lapse:** Equifax critically failed to patch the known vulnerability within a reasonable timeframe, exposing its system for months. This highlights a need for more effective vulnerability management practices.
- **Inadequate IAM (Identity and Access Management) Policies:** The presence of weak access controls granted excessive privileges to unauthorized users, significantly increasing the attack surface. This signifies a failure to implement the principle of least privilege.

  - Enforcing MFA (Multi-Factor Authentication) adds an extra layer of security by requiring a second verification factor beyond just a username and password.

  Role-based access Control (RBAC) assigns access permission based on predefined roles within the organization. This ensures that users only have access to resources aligned with their designated duties. In the Equifax breach, if access to the vulnerable system were limited to authorized personnel with specific roles, the attacker's ability to exploit the vulnerability would have been significantly low.

- **Insufficient Awareness and Training:** The incident suggests a potential lack of cybersecurity awareness training for employees, leaving them susceptible to social engineering attacks or falling victim to phishing attempts.

How did it happen?

- The company was hacked via a consumer complaint web portal, and a vulnerability, dubbed CVE-2017-5638, was discovered in Apache Struts, an open-source web framework.
- Equifax's investigation of the breach identified four significant factors: identification, detection, segmentation of access to databases, and data governance, which allowed the attacker to successfully gain access to its network and extract information from PII databases.
- The crisis began in March 2017. A vulnerability was found in Apache Struts, and the Apache Software Foundation released a patch for it. On March 9, Equifax admins were told to apply the patch to any affected systems, but the employee who should have done so didn't.

(Part 2)

Defensive Lapses and Network Administration Issues

- **Security Information and Event Management (SIEM) Ineffectiveness:** The absence of robust SIEM tools or inadequate monitoring procedures likely resulted in delayed intrusion detection.
- **Insufficient Network Segmentation:** A segmented network could have contained the breach's scope, minimizing the attackers' lateral movement within the system.
- **Vulnerability Management:** Equifax failed to prioritize timely patching of known vulnerabilities, leaving their system susceptible to exploitation.
- **Access Controls:** Inadequate access controls might have allowed attackers to move laterally within the network after gaining initial access.
- **Data Minimization:** Equifax reportedly held onto more data than necessary, increasing the potential impact of the breach.
- **Patch Management:** Implement a rigorous system for timely patching of known vulnerabilities.
- **Multi-Factor Authentication (MFA):** Enforce robust authentication protocols like MFA to add an extra layer of security.
- **Continuous Monitoring:** Implement robust intrusion detection and prevention systems (IDS/IPS) to monitor network activity for suspicious behavior.

The Equifax breach exposed significant shortcomings in their cybersecurity risk management practices, deviating from the core principles of the NIST CSF:

- **Identify:** Equifax reportedly failed to maintain a complete IT asset inventory, hindering their ability to identify the vulnerable application (Apache Struts) on their network.
- **Protect:** A known vulnerability **(CVE-2017-5638)** in the Apache Struts software remained unpatched for months, exposing the system.
- **Detect:** Equifax lacked adequate intrusion detection and prevention systems, allowing the attackers to operate undetected for a significant period.

Major/Outstanding Causes:
- A known vulnerability that wasn't patched promptly
- Insufficient resources or processes dedicated to security maintenance
- Inadequate security awareness and training

Systems Vulnerable to Attack:
- Web application for consumers' credit score checks
- Apache Struts, an open-source web framework
- CVE-2017-5638, a publicly known vulnerability in the Apache Struts Software

Steps that Equifax could take to:
- Prevent the Breach:

1. Patching vulnerabilities promptly
2. Get the basics right
3. Robust security practices
4. Data minimization and Governance
5. Employee training

(Part 3)

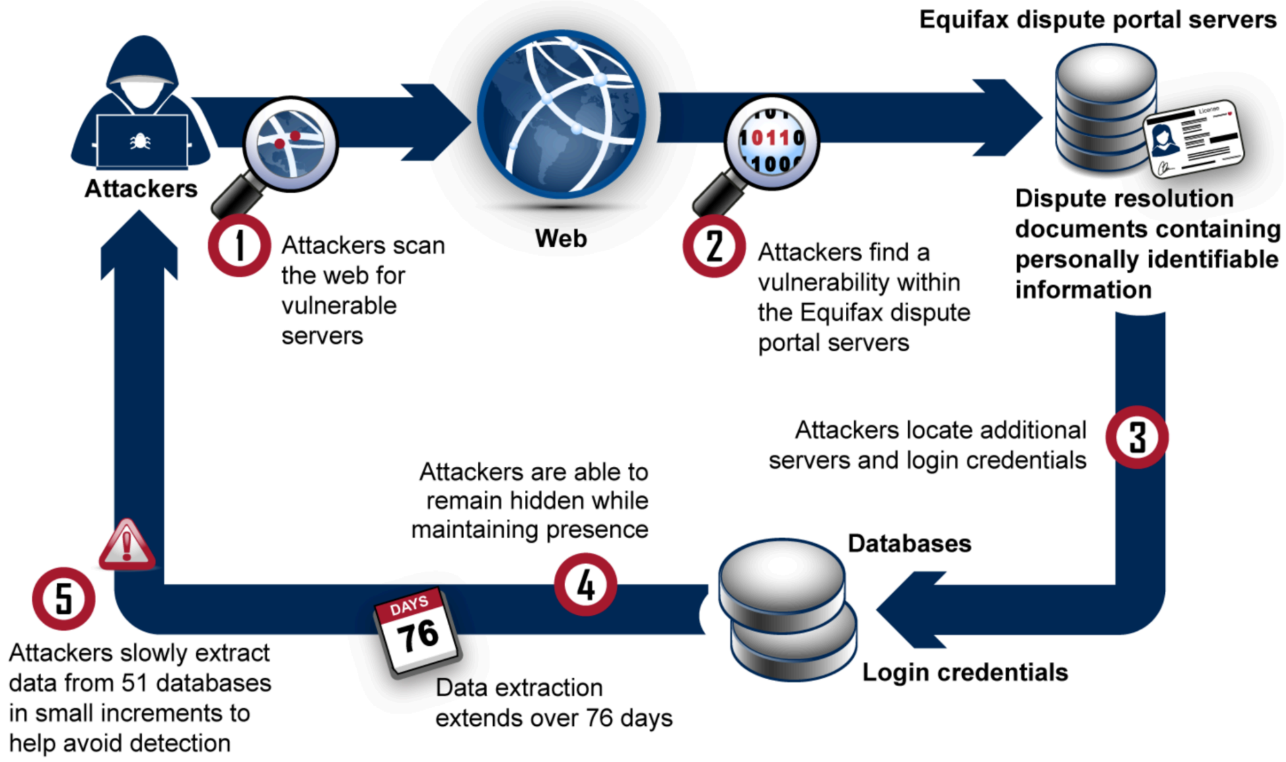
Offensive Cybersecurity

From an offensive cybersecurity perspective, the Equifax breach demonstrates the importance of threat intelligence and penetration testing. Equifax failed to detect the vulnerability in its system despite the availability of threat intelligence indicating the potential for exploitation. Additionally, Equifax's reliance on outdated and ineffective security measures, such as static passwords, highlights the importance of regularly testing and updating security controls to adapt to evolving threats.

Equifax Response:

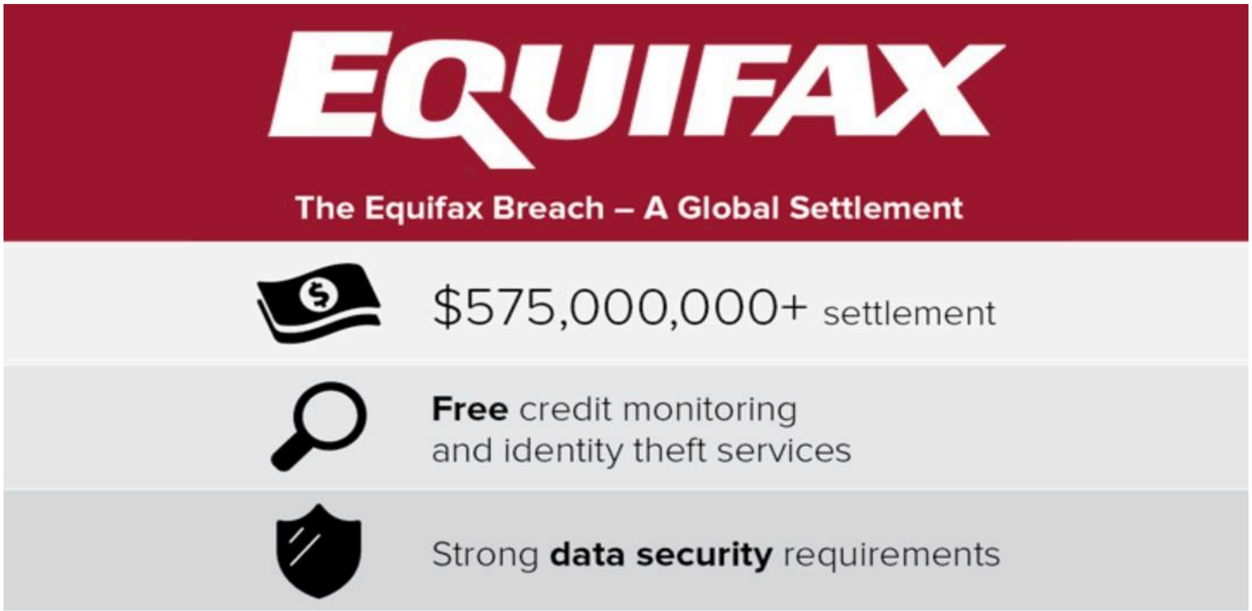
Equifax's assessment of the data breach began with action taken to identify that it was being attacked and subsequent action to block the intrusion. Equifax officials publicly announced the breach approximately 2.5 months after the attackers began extracting sensitive data on May 13, 2017. A network admin conducting routine checks of IT systems' operating status and configurations discovered that a misconfigured piece of equipment allowed attackers to communicate with compromised servers and steal data without detection.

How Attackers Exploited Vulnerabilities in the 2017 Breach, Based on Equifax Information


Equifax dispute portal servers
Attackers
Web
1 Attackers scan the web for vulnerable servers
2 Attackers find a vulnerability within the Equifax dispute portal servers
1011
100
Dispute resolution documents containing personally identifiable information
3 Attackers locate additional servers and login credentials
Databases
Login credentials
4 Attackers are able to remain hidden while maintaining presence
DAYS
76
Data extraction extends over 76 days
5 Attackers slowly extract data from 51 databases in small increments to help avoid detection

Source: GAO, based on information provided by Equifax. | GAO-18-559

- Equifax was breached by Chinese state-sponsored hackers whose purpose was espionage, not theft.
- Equifax must pay $700 million in fines to settle a series of state and federal investigations into the massive 2017 data breach.



EQUIFAX

The Equifax Breach – A Global Settlement

$575,000,000+ settlement

Free credit monitoring
and identity theft services

Strong **data security** requirements

Offensive Techniques Employed

The attackers employed techniques like:

- **Social Engineering:** Phishing emails or social media manipulation have been used to gain initial access credentials.
- **Exploit Kits:** Automated tools readily available online could have been used to exploit the unpatched vulnerability in the Apache Struts software.
- **Lateral Movement:** Once inside the network, attackers have used various techniques to move laterally and access sensitive data.

Penetration testing, a core principle of Offensive Cybersecurity, could have identified the vulnerability before malicious actors exploited it.

Equifax's major missteps in response to the attack that caused further damage:

- Misdirecting consumers to a fraudulent website
- Requiring additional information for verification
- Delay public notification and lack of transparency
- Inadequate compensation and assistance for affected individuals

Steps that Equifax could take to:
- Mitigating the Impact:

1. Early detection and response
2. Transparent communication
3. Offering effective safeguards
4. Regular security audits and assessments

As the head of the response team, I would recommend the following:

- **Prioritize transparency**
    1. Early public disclosure and clear
    2. consistent communication
- **Protect Consumers and Minimize Further Damage**
    1. Secure the vulnerable system immediately
    2. Offer robust credit monitoring and identify theft protection
    3. Do not require additional sensitive information
- **Cooperate with Authorities and Enhance Security Measures:**
    1. Fully cooperate with law enforcement
    2. Conduct a thorough post-incident review
- **Take Responsibility and Offer Adequate Compensation:**
    1. Offer fair and appropriate compensation
    2. Acknowledge the severity of the breach and take full responsibility

What Lessons We Learned from the Equifax Data Breach:

- Prioritize Patching Vulnerabilities
- Implement Robust Security Practices
- Minimize Data Collection and Storage
- Network Segmentation
- Have a Defined Incident response plan
- Invest in Security Measures
- Communicate Transparently and Proactively
- Penetration Testing
- Vulnerability Scanning

Resources:

Equifax data breach FAQ: What happened, who was affected, what was the impact? | CSO Online
EPIC - Equifax Data Breach
2017 Equifax data breach - Wikipedia
Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach
Case Study: Equifax Data Breach - Seven Pillars Institute
Equifax to Pay up to $700 Million in 2017 Data Breach Settlement
NVD - cve-2017-5638